Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard

Wen, Long; Wang, Meiqin; Bogdanov, Andrey; Chen, Huaifeng

Published in:
Information Processing Letters

Link to article, DOI:
10.1016/j.ipl.2014.01.007

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

Information Processing Letters 114 (2014) 322–330

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard

Long Wen [a], Meiqin Wang [a,*], Andrey Bogdanov [b,*], Huaifeng Chen [a]

[a] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[b] Technical University of Denmark, Denmark

ARTICLE INFO

Article history:
Received 6 August 2013
Received in revised form 20 November 2013
Accepted 20 January 2014
Available online 21 January 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Analysis of algorithms
Block cipher
Zero-correlation linear cryptanalysis
HIGHT

ABSTRACT

HIGHT is a block cipher designed in Korea with the involvement of Korea Information Security Agency. It was proposed at CHES 2006 for usage in lightweight applications such as sensor networks and RFID tags. Lately, it has been adopted as ISO standard. Though there is a great deal of cryptanalytic results on HIGHT, its security evaluation against the recent zero-correlation linear attacks is still lacking. At the same time, the Feistel-type structure of HIGHT suggests that it might be susceptible to this type of cryptanalysis. In this paper, we aim to bridge this gap.

We identify zero-correlation linear approximations over 16 rounds of HIGHT. Based upon those, we attack 27-round HIGHT (round 4 to round 30) with improved time complexity and practical memory requirements. This attack of ours is the best result on HIGHT to date in the classical single-key setting. We also provide the first attack on 26-round HIGHT (round 4 to round 29) with the full whitening key.

1. Introduction

1.1. Lightweight block ciphers, HIGHT, and existing cryptanalysis

With emerging pervasive applications in mind such as sensor networks, RFID tags and medical devices, a variety of lightweight cryptographic algorithms have been lately proposed including the two block ciphers adopted as ISO/IEC standard for lightweight encryption: PRESENT [7] proposed at CHES 2007 and CLEFIA [8] proposed at FSE 2007. Many more lightweight block ciphers have been published since then. Even the U.S. National Security Agency (NSA) has very recently contributed to the trend with two lightweight block ciphers: Simon and Speck [1]. HIGHT [6] is another lightweight block cipher designed with governmental involvement – Korea Information Security Agency (KISA).

HIGHT was proposed at CHES 2006 and then adopted as ISO standard block cipher [9]. HIGHT has 32 rounds. It accepts a 64-bit block and a 128-bit key. Each round consists of four parallel Feistel functions. Whitening keys are applied before the first and after the last round. The security of HIGHT has been extensively evaluated. Zhang et al. [10] present an integral attack on 22-round HIGHT at CANS 2009 and the time complexity is then reduced by Sasaki and Wang [11] at SAC 2012. In the impossible differential cryptanalysis of HIGHT, to be able to cryptanalyze more rounds, most of the existing attacks do not consider the pre-whitening key except the attack on 27-round HIGHT given in [14] at AfricaCrypt 2012. Lu [12] gives the first impossible differential cryptanalysis against 25-round HIGHT. Then at ACISP 2009, Özen et al. [13] successfully

* Corresponding authors.
E-mail addresses: mqwang@sdu.edu.cn (M. Wang), anbog@dtu.dk (A. Bogdanov).

http://dx.doi.org/10.1016/j.ipl.2014.01.007

Table 1
Summary of **single-key** attacks on HIGHT.

Attack	Rounds	Pre./Post.	Data	Time	Memory	Ref.
IA	22 (1∼22)	✓/✓	2^{62} CPs	$2^{118.71}$ ENs	2^{64} Bytes	[10]
IA	22 (1∼22)	✓/✓	2^{62} CPs	$2^{102.35}$ ENs	2^{64} Bytes	[11]
ID	25 (6∼30)	–/✓	2^{60} CPs	$2^{126.78}$ ENs	N/A	[12]
ID	26 (1∼26)	–/✓	2^{61} CPs	$2^{119.53}$ ENs	2^{109} Bytes	[13]
ID	26 (5∼30)	–/✓	$2^{61.6}$ CP	$2^{114.35}$ ENs	$2^{87.6}$ Bytes	[14]
ZC	**26** (4∼29)	✓/✓	$2^{62.79}$ **KPs**	$2^{119.1}$ **ENs**	2^{43} **Bytes**	**Section 4.1**
ID	27 (4∼30)	✓/✓	2^{58} CPs	$2^{126.6}$ ENs $+2^{120}$ MAs	2^{120} Bytes	[14]
ZC	**27** (4∼30)	✓/✓	$2^{62.79}$ **KPs**	$2^{120.78}$ **ENs**	2^{43} **Bytes**	**Section 4.2**

IA: Integral Attack; ID: Impossible Differential; ZC: Zero-Correlation Linear; Pre.: Pre-Whitening; Post.: Post-Whitening; CP: Chosen Plaintext; KP: Known Plaintext; MA: Memory Access; EN: Encryption.

mount an impossible differential attack on 26-round HIGHT. This result was then improved by Chen et al. [14] at AfricaCrypt 2012. Note that the attack on 27-round HIGHT with full whitening keys considered proposed in [14] has time complexity $2^{126.6}$ encryptions and 2^{120} memory accesses to a table of 2^{120} bytes, which can be considered marginal with respect to brute force. In the related-key setting, attacks on 28-round [12] and 31-round [13] HIGHT were presented using impossible differential attack and related-key rectangle attack on the full HIGHT was reported in [17]. Recently, independent biclique attacks – belonging to the class of polynomial advantage attacks – on the full HIGHT have been obtained in [15,16] with time complexities $2^{126.4}$ and $2^{125.9}$ encryptions, respectively.

1.2. Zero-correlation cryptanalysis

Zero-correlation linear cryptanalysis proposed by Bogdanov and Rijmen in [4] is a novel promising attack technique for block ciphers which has its theoretical foundation in the availability of numerous key-independent unbiased linear approximations with correlation zero for many ciphers. (If p is the probability for a linear approximation to hold, its correlation is defined as $c = 2p - 1$.) Though the initial distinguisher of [4] had some limitations in terms of data complexity, they were overcome in the FSE 2012 paper [5], where the existence of multiple linear approximations with correlation zero in target ciphers was used to propose a more data-efficient distinguisher. In a follow-up work at AsiaCrypt 2012 [2], fundamental links of integral cryptanalysis to zero-correlation cryptanalysis have been revealed. Namely, integrals (similar to saturation or multiset distinguishers) have been demonstrated to be essentially a special case of the zero-correlation property. On top of that, a multidimensional distinguisher has been constructed for the zero-correlation property, which removed the unnecessary independency assumptions on the distinguishing side. At SAC 2013 [3], an FFT technique for speeding up the key recovery in zero-correlation attacks has been proposed, which resulted in increasing the number of rounds that can be cryptanalyzed for Camellia-128 and Camellia-192 in the single-key setting.

1.3. Our contributions

In this paper, we evaluate the security of HIGHT with respect to the recent technique of zero-correlation linear cryptanalysis. Our contributions can be summarized as follows.

1. We reveal 16-round linear approximations of correlation zero in HIGHT.
2. Based on those approximations, we propose a multidimensional zero-correlation attack on 27 rounds of HIGHT (round 4 to round 30) with all whitening keys. As mentioned above, in the single-key setting, the attack on the highest number of HIGHT rounds is the 27-round impossible differential attack of [14]. However, the latter provides only a marginal improvement over the brute force, given the enormous number of random accesses to a huge memory (see Table 1). Our zero-correlation attack features a lower time complexity that does not involve expensive memory accesses and a significantly reduced memory complexity, which is in fact practical. Our attack is arguably the best non-exhaustive attack on HIGHT in the classical single-key setting.
3. We provide a key-recovery attack on 26-round HIGHT (round 4 to round 29) with all whitening keys. Note that all previous attacks on 26-round HIGHT ignored the pre-whitening key. To do this, we use the technique of multidimensional zero-correlation linear cryptanalysis. Thus, this attack of ours is the first one on 26-round HIGHT with all whitening keys in the single secret key setting.

Our results along with the previous attacks on HIGHT are shown in Table 1.

1.4. Outline

This paper is organized as follows. Section 2 briefly describes HIGHT and outlines the ideas of zero-correlation linear cryptanalysis. Section 3 presents our zero-correlation linear approximations that span 16 rounds of HIGHT. Section 4 illustrates our attacks on 26-round and 27-round HIGHT. We conclude in Section 5.

2. Preliminaries

2.1. Notation

$\boxplus$: addition modular 2^8
$\oplus$: exclusive-OR (XOR)
P_i, C_i: the i-th byte of plaintext and ciphertext, $0 \leqslant i \leqslant 7$

Algorithm 1 Key schedule of HIGHT.

$WK_0 = MK_{12}$, $WK_1 = MK_{13}$, $WK_2 = MK_{14}$, $WK_3 = MK_{15}$
$WK_5 = MK_0$, $WK_5 = MK_1$, $WK_6 = MK_2$, $WK_7 = MK_3$
$s_0 = 0$, $s_1 = 1$, $s_2 = 0$, $s_3 = 1$, $s_4 = 1$, $s_5 = 0$, $s_6 = 1$
$\delta_0 = s_6|s_5|s_4|s_3|s_2|s_1|s_0$
for $i = 1 \to 127$ **do**
  $s_{i+6} = s_{i+1} \oplus s_{i-1}$
  $\delta_i = s_{i+6}|s_{i+5}|s_{i+4}|s_{i+3}|s_{i+2}|s_{i+1}|s_i$
end for
for $i = 0 \to 7$ **do**
  for $j = 0 \to 7$ **do**
    $SK_{16i+j} = MK_{(j-i) mod 8} \boxplus \delta_{16i+j}$
  end for
  for $j = 0 \to 7$ **do**
    $SK_{16i+j+8} = MK_{((j-i) mod 8)+8} \boxplus \delta_{16i+j+8}$
  end for
end for

X^r: the input value of round r, $1 \leqslant r \leqslant 32$
X_i^r: the i-th byte of X^r, $0 \leqslant i \leqslant 7$, corresponding to eight branches
$X_{i(j)}^r$: the j-th bit of X_i^r, $0 \leqslant j \leqslant 7$
MK_i: the i-th master key byte, $0 \leqslant i \leqslant 15$
WK_i: the i-th whitening key, $0 \leqslant i \leqslant 7$
SK_i: the i-th subkey, $0 \leqslant i \leqslant 127$
$\lll s$: cyclic left shift by s bits, $0 \leqslant s \leqslant 7$
$|$: concatenation of bits or bytes

2.2. Description of HIGHT

HIGHT is a 32-round lightweight block cipher with a 64-bit block and a 128-bit master key. It is an 8-line type-II generalized Feistel network: Each round consists of four parallel applications of F_0 and F_1 functions. Whitening keys are added before the first and after the last round. The 16-byte master key is denoted as $(MK_{15}, MK_{14}, \ldots, MK_0)$; the eight whitening key bytes are given by $(WK_7, WK_6, \ldots, WK_0)$; we address the 128 subkey bytes by $(SK_{127}, SK_{126}, \ldots, SK_0)$. Both the whitening keys and subkeys are generated from the master key by the key schedule shown in Algorithm 1. Both the whitening keys and subkeys are generated from the master key. The relation between master key bytes and partial subkeys and whitening keys are shown in Table 2.

The 64-bit plaintext P and ciphertext C are denoted as $(P_7|\cdots|P_0)$ and $(C_7|\cdots|C_0)$, respectively. The 64-bit input X^i of round i is denoted as $(X_7^i|\cdots|X_0^i)$. The encryption process of HIGHT is shown in Algorithm 2, in which $F_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7)$ and $F_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6)$.

Algorithm 2 Encryption process of HIGHT.

// Pre-Whitening
$X_7^0 = P_7, X_6^0 = P_6 \oplus WK_3$, $X_5^0 = P_5$, $X_4^0 = P_4 \boxplus WK_2$
$X_3^0 = P_3$, $X_2^0 = P_2 \oplus WK_1$, $X_1^0 = P_1$, $X_0^0 = P_0 \boxplus WK_0$
for $i = 0 \to 30$ **do**
  $X_7^{i+1} = X_6^i$, $X_6^{i+1} = X_5^i \boxplus (F_1(X_4^i) \oplus SK_{4i+2})$
  $X_5^{i+1} = X_4^i$, $X_4^{i+1} = X_3^i \oplus (F_0(X_2^i) \boxplus SK_{4i+1})$
  $X_3^{i+1} = X_2^i$, $X_2^{i+1} = X_1^i \boxplus (F_1(X_0^i) \oplus SK_{4i})$
  $X_1^{i+1} = X_0^i$, $X_0^{i+1} = X_7^i \oplus (F_0(X_6^i) \boxplus SK_{4i+3})$
end for
for $i = 31$ **do**
  $X_7^{i+1} = X_7^i \oplus (F_0(X_6^i) \boxplus SK_{127})$, $X_6^{i+1} = X_6^i$
  $X_5^{i+1} = X_5^i \boxplus (F_1(X_4^i) \oplus SK_{126})$, $X_4^{i+1} = X_4^i$
  $X_3^{i+1} = X_3^i \oplus (F_0(X_2^i) \boxplus SK_{125})$, $X_2^{i+1} = X_2^i$
  $X_1^{i+1} = X_1^i \boxplus (F_1(X_0^i) \oplus SK_{124})$, $X_0^{i+1} = X_0^i$
end for
// Post-Whitening
$C_7 = X_7^{32}$, $C_6 = X_6^{32} \oplus WK_7$, $C_5 = X_5^{32}$, $C_4 = X_4^{32} \boxplus WK_6$
$C_3 = X_3^{32}$, $C_2 = X_2^{32} \oplus WK_5$, $C_1 = X_1^{32}$, $C_0 = X_0^{32} \boxplus WK_4$

2.3. Zero-correlation linear cryptanalysis

In this section, we briefly recall the basic concepts of zero-correlation linear cryptanalysis based on [4] and [2].

First, we briefly mention the concept of correlation for linear approximations. We denote the scalar product of binary vectors by $a \diamond x = \bigoplus_{i=1}^{n} a_i x_i$. Linear cryptanalysis is based on linear approximations determined by input mask α and output mask β. A linear approximation $\alpha \to \beta$ of a vectorial function f has a correlation defined by

$$C\big(\beta \diamond f(x), \alpha \diamond x\big) = 2 \Pr_x\big(\beta \diamond f(x) \oplus \alpha \diamond x = 0\big) - 1.$$

In zero-correlation linear cryptanalysis, the distinguisher uses linear approximations with zero correlation for all keys while the classical linear cryptanalysis utilizes linear approximations with correlation as far from zero as possible.

In [2], Bogdanov et al. proposed a multidimensional zero-correlation linear distinguisher using ℓ zero-correlation linear approximations and requiring $\mathcal{O}(2^n/\sqrt{\ell})$ known plaintexts, where n is the block size of a cipher.

Table 2
Partial key relation of HIGHT.

R	Subkey used			
Pre.	$WK_3(MK_{15})$	$WK_2(MK_{14})$	$WK_1(MK_{13})$	$WK_0(MK_{12})$
4	$SK_{15}(MK_{15})$	$SK_{14}(MK_{14})$	$SK_{13}(MK_{13})$	$SK_{12}(MK_{12})$
5	$SK_{19}(MK_2)$	$SK_{18}(MK_1)$	$SK_{17}(MK_0)$	$SK_{16}(MK_7)$
6	$SK_{23}(MK_6)$	$SK_{22}(MK_5)$	$SK_{21}(MK_4)$	$SK_{20}(MK_3)$
7	$SK_{27}(MK_{10})$	$SK_{26}(MK_9)$	$SK_{25}(MK_8)$	$SK_{24}(MK_{15})$
8	$SK_{31}(MK_{14})$	$SK_{30}(MK_{13})$	$SK_{29}(MK_{12})$	$SK_{28}(MK_{11})$
9	$SK_{35}(MK_1)$	$SK_{34}(MK_0)$	$SK_{33}(MK_7)$	$SK_{32}(MK_6)$
…	…	…	…	…
26	$SK_{103}(MK_1)$	$SK_{102}(MK_0)$	$SK_{101}(MK_7)$	$SK_{100}(MK_6)$
27	$SK_{107}(MK_{13})$	$SK_{106}(MK_{12})$	$SK_{105}(MK_{11})$	$SK_{104}(MK_{10})$
28	$SK_{111}(MK_9)$	$SK_{110}(MK_8)$	$SK_{109}(MK_{15})$	$SK_{108}(MK_{14})$
29	$SK_{115}(MK_4)$	$SK_{114}(MK_3)$	$SK_{113}(MK_2)$	$SK_{112}(MK_1)$
30	$SK_{119}(MK_0)$	$SK_{118}(MK_7)$	$SK_{117}(MK_6)$	$SK_{116}(MK_5)$
Post.	$WK_7(MK_3)$	$WK_6(MK_2)$	$WK_5(MK_1)$	$WK_4(MK_0)$

Table 3
Zero-correlation linear approximations for 16-round HIGHT.

r	Γ_7^r	Γ_6^r	Γ_5^r	Γ_4^r	Γ_3^r	Γ_2^r	Γ_1^r	Γ_0^r
↓1	0	0	0	00000001	0	0	0	0
2	0	0	00000001	0	0	0	0	0
3	0	00000001	00110100	0	0	0	0	0
4	00000001	001?????	?	0	0	0	0	0
5	111?????	?	?	0	0	0	0	00000001
6	?	?	?	0	0	0	00000001	111?????
7	?	?	?	0	0	00000001	110?????	?
8	?	?	?	0	00000001	1???????	?	?
9	?	?	?	00000001	**0**???????	?	?	?
9	?	?	?	?	**1**???????	?	?	?
10	?	?	0	1???????	?	?	?	?
11	0	0	1???????	?	?	?	?	?
12	0	1???????	?	?	?	?	0	0
13	1???????	?	?	?	0	0	0	0
14	?	?	0	0	0	0	0	1???????
15	0	0	0	0	0	0	1???????	?
16	0	0	0	0	0	1???????	0	0
↑17	0	0	0	0	1???????	0	0	0

In multidimensional zero-correlation cryptanalysis, the key recovery works as follows. For an n-bit block cipher, if there are m independent zero-correlation linear approximations such that all $\ell = 2^m$ non-zero linear combinations of them have zero correlation, the number of required known plaintexts N is $\mathcal{O}(2^n/\sqrt{\ell})$. For each of the 2^m values $z \in \mathbb{F}_2^m$, the attacker initializes a counter $V[z]$, $z = 0, 1, 2, \ldots, 2^m - 1$, to value zero. The attacker partially encrypts and decrypts each plaintext-ciphertext pair to the boundaries of zero-correlation linear approximations by guessing some key values and computes the corresponding data value in $\mathbb{F}_2^m$ by evaluating the m basis linear approximations and increments the counter $V[z]$ of this data value by one. Then the attacker computes the statistic T:

$$T = \sum_{z=0}^{2^m-1} \frac{(V[z] - N2^{-m})^2}{N2^{-m}(1-2^{-m})}.$$

The statistic T for the right key guess follows a χ^2 distribution with mean $\mu_0 = (\ell - 1)\frac{2^n - N}{2^n - 1}$ and variance $\sigma_0^2 = 2(\ell - 1)(\frac{2^n - N}{2^n - 1})^2$, while for the wrong key guess it follows a χ^2-distribution with mean $\mu_1 = \ell - 1$ and variance $\sigma_1^2 = 2(\ell - 1)$.

We denote the type-I error probability as α_0 (the probability to wrongfully discard the right key guess), the type-II error probability as α_1 (the probability to wrongfully accept a wrong key guess as the right key). If we consider the decision threshold $\tau = \mu_0 + \sigma_0 q_{1-\alpha_0} = \mu_1 - \sigma_1 q_{1-\alpha_1}$, then the number of distinct known plaintexts is

$$N = \frac{(2^n - 1)(q_{1-\alpha_0} + q_{1-\alpha_1})}{\sqrt{(\ell - 1)/2} + q_{1-\alpha_0}} + 1,$$

where $q_{1-\alpha_0}$ and $q_{1-\alpha_1}$ are the respective quantiles of the standard normal distribution.

3. Zero-correlation linear approximations of 16-round HIGHT

To discuss the linear approximations, we need a proper way to denote linear masks. Hence, in the rest of the paper, if a mask on one byte is zero or undetermined in all 8 bits, we denote it with a single '0' or '?', respectively. Otherwise, we will refer to this mask bit by bit where '0', '1' and '?' stand for a zero, nonzero and undetermined single-bit mask value.

Based on properties of correlation for linear approximations over basic operations used in HIGHT such as linear map, XOR, branching, and modular addition proposed in [4,5], we derive a variety of zero-correlation linear approximations for 16-round HIGHT.

Theorem 1. *Denote the input mask as* $\alpha = (\alpha_7, \alpha_6, \ldots, \alpha_0)$ *and output mask after* 16 *rounds of HIGHT as* $\beta = (\beta_7, \beta_6, \ldots, \beta_0)$. *For any* $\alpha_i = 00000001$, $\alpha_j = 0$, $j \neq i$, $0 \leqslant i, j \leqslant 7$, $\beta_k = 1???????$, $\beta_l = 0$, $l \neq k$, $0 \leqslant l, k \leqslant 7$, *if* $(i,k) \in \{(6,5), (4,3), (2,1), (0,7)\}$, *then the linear approximations* $\alpha \xrightarrow{16r} \beta$ *have correlation zero. For each* $(i,k) \in \{(6,5), (4,3), (2,1), (0,7)\}$, *there exist* 128 *linear approximations conforming to* $\alpha \xrightarrow{16r} \beta$.

Due to limited space here, we do not provide the proof of Theorem 1. However, we list the details of the zero-correlation linear approximations over 16-round HIGHT when $(i,k) = (4,3)$ in Table 3 since this kind of linear approximations will be used in our attack.

4. Key-recovery attack on 26/27-round HIGHT

In this section, we describe our attacks on 26 and 27 rounds of HIGHT. We use the key schedule of HIGHT to reduce the number of guessed bits in our attack. The number of guessed key bits is affected by several parameters including the zero-correlation linear property we choose (values of α and β), the position of the property (rounds spanned by zero-correlation approximations), and

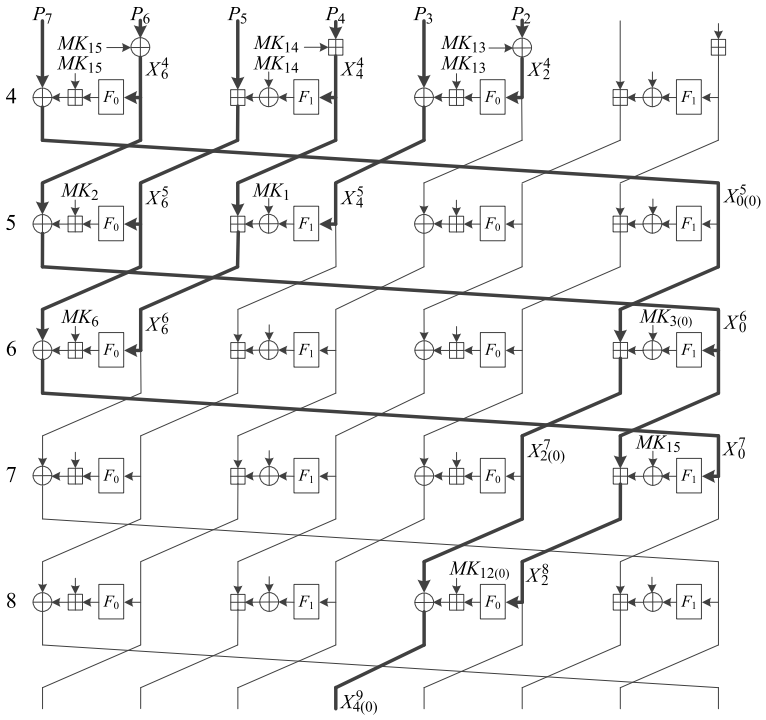

Fig. 1. Initial five rounds encryption.

the number of rounds added before and after this property. To optimize the attack complexities, a proper choice of these parameters is needed. We have implemented the search for the best parameters in a computer program which counts the number of guessed key bits in the partial encryption/decryption phase for all possible combinations of the parameters. To reduce the time complexity, we choose parameters with the least number of guessed key bits.

As a result, we can attack 26-round HIGHT (round 4 to round 29) with the full whitening key by spanning rounds 9 to 24 with the 16-round zero-correlation linear property of Theorem 1 and adding five rounds before and after the property. Also we can attack 27-round HIGHT (round 4 to round 30) with the full whitening key if we add five rounds before and six rounds after the zero-correlation property. We provide our attacks on 26- and 27-round HIGHT in Sections 4.1 and 4.2, respectively.

4.1. Key-recovery attack on 26-round HIGHT

The five initial rounds and five final rounds involved in the attack on 26-round HIGHT are shown in Fig. 1 and Fig. 2, respectively. We need to encrypt and decrypt N (P, C) pairs to the boundaries of those zero-correlation linear approximations. In Fig. 1 and Fig. 2, we only show those intermediate state values, the subkeys, and whitening keys computed or guessed in the partial encryption and decryption process. The guessed subkeys and whitening keys are denoted with their corresponding master key bytes. Then the key-recovery attack on 26-round HIGHT is proceeded with partial-sum technique from Step 1 to Step 16 as follows.

1. Allocate a counter vector $V_1[X^9_{4(0)}|C_7|C_6|C_5|C_4|X^{29}_3]$ of size 2^{41} where each element is 32-bit length and initialize to zero.
2. Guess all possible values of 50 master key bits MK_{15}, MK_{14}, MK_{13}, MK_2, MK_1, MK_6, $MK_{3(0)}$, $MK_{12(0)}$.
3. Partially encrypt and decrypt each of N (P, C) pairs to get $X^9_{4(0)}$ and X^{29}_3 (e.g. $X^{29}_3 = C_3 \oplus (F_0(C_2 \oplus WK_5) \boxplus SK_{113})$). Add one to the corresponding $V_1[X^9_{4(0)}|C_7|C_6|C_5|C_4|X^{29}_3]$.

The time complexity of Step 3 is no more than $N \cdot 2^{50} \cdot \frac{5}{26}$ 26-round encryptions. Then, we proceed Steps 4–13 shown in Table 4. The second column stands for the master key byte or bit that should be guessed in each step and the corresponding subkey or whitening key is listed in the third column. The column headed as "#Bits" denotes the number of new guessed master key bits introduced in each step. The fifth column is the state value to be computed with the guessed key and known state value. We set up counters in each step to reduce time complexity. The counters we set are shown in column headed as "Counter" and its size is shown in the next column head as "Size". The computational complexity of each step is shown in the last column, measured with 1/4 round encryption except those steps noted with '†'.

To be more clear we explain Step 4 of Table 4 in details. In Step 4 of Table 4, we set up a counter vector $V_2[X^9_{4(0)}|C_7|C_6|C_5|X^{29}_4|X^{29}_3]$ of size 2^{41} where each element is 32-bit length and initialize to zero and guess master key byte MK_2 corresponding to WK_6. There is no new master key bits introduced since the value of MK_2 has already been guessed in Step 2. Compute $C_4 \boxplus WK_6 \rightarrow X^{29}_4$

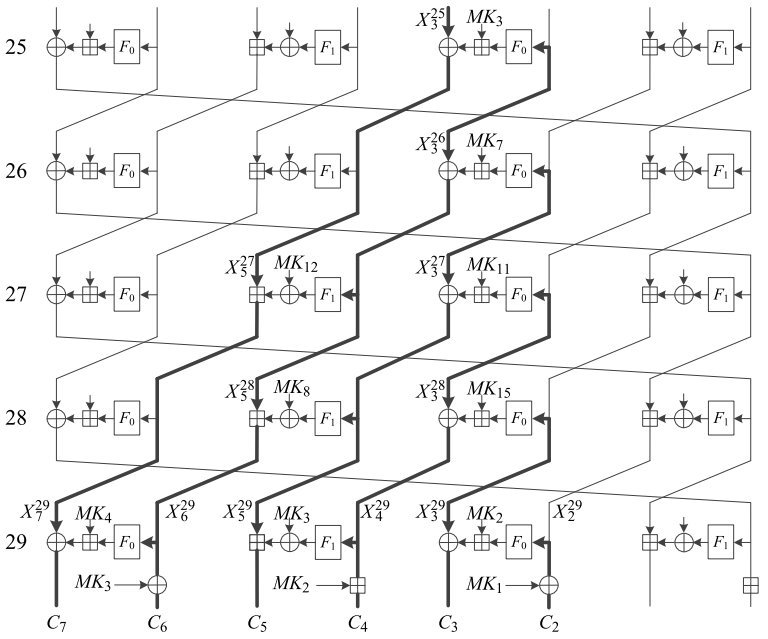

Fig. 2. Final five rounds decryption.

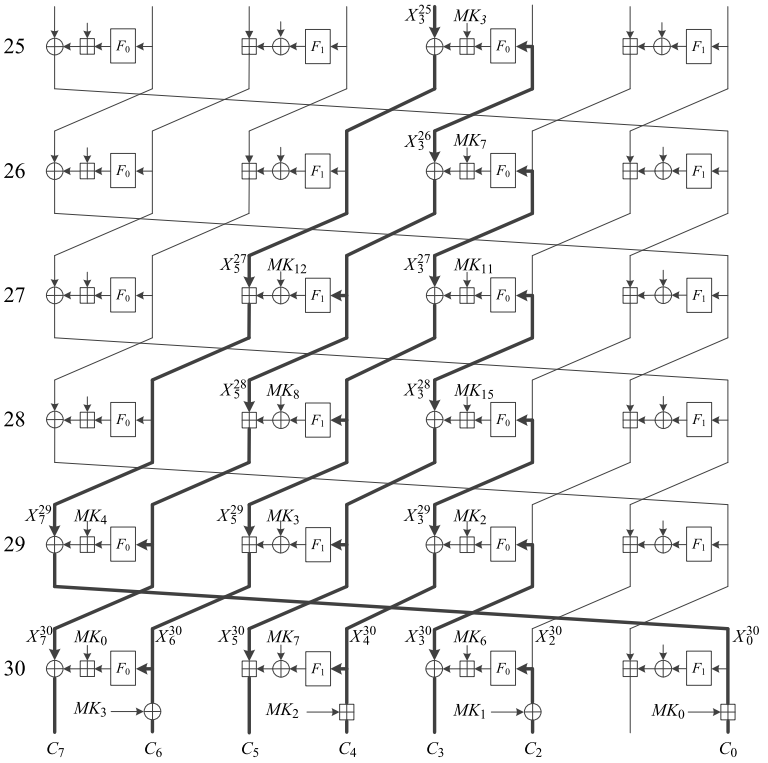

Fig. 3. Final six rounds decryption.

and add the corresponding $V_1[X_{4(0)}^9|C_7|C_6|C_5|C_4|X_3^{29}]$ to $V_2[X_{4(0)}^9|C_7|C_6|C_5|X_4^{29}|X_3^{29}]$. Step 5 to Step 13 are proceeded in a similar way and after Step 13 we get the counters $V_{11}[X_{4(0)}^9|X_3^{25}]$ for all possible values of $(X_{4(0)}^9|X_3^{25})$.

Note that to reduce the time complexity of Step 12 of Table 4, we guess the key byte of MK_7 bit by bit, from the least significant bit to the most significant bit. The detailed procedure is shown in Table 5. The columns in Table 5

Table 4
Partial decryption procedure of the attack on 26-round HIGHT.

Step	Guess	Known key	#Bits	Computing	Counter	Size	Comp.
4	MK_2	WK_6	0	$C_4 \boxplus WK_6 \to X_4^{29}$	$V_2[X_{4(0)}^9 \| C_7 \| C_6 \| C_5 \| X_4^{29} \| X_3^{29}]$	41	$2^{41} \cdot 2^{50\dagger}$
5	$MK_{3(7\sim1)}{}^*$	$SK_{114(7\sim1)}$	7	$C_5 \boxminus (F_1(X_4^{29}) \oplus SK_{114}) \to X_5^{29}$	$V_3[X_{4(0)}^9 \| C_7 \| C_6 \| X_5^{29} \| X_4^{29} \| X_3^{29}]$	41	$2^{41} \cdot 2^{57}$
6	MK_{15}	SK_{109}	0	$X_4^{29} \oplus (F_0(X_3^{29}) \boxplus SK_{109}) \to X_3^{28}$	$V_4[X_{4(0)}^9 \| C_7 \| C_6 \| X_5^{29} \| X_3^{28}]$	33	$2^{41} \cdot 2^{57}$
7	MK_3	WK_7	0	$C_6 \oplus WK_7 \to X_6^{29}$	$V_5[X_{4(0)}^9 \| C_7 \| X_6^{29} \| X_5^{29} \| X_3^{28}]$	33	$2^{33} \cdot 2^{57\dagger}$
8	MK_4	SK_{115}	8	$C_7 \oplus (F_0(X_6^{29}) \boxplus SK_{115}) \to X_7^{29}$	$V_6[X_{4(0)}^9 \| X_7^{29} \| X_6^{29} \| X_5^{29} \| X_3^{28}]$	33	$2^{33} \cdot 2^{65}$
9	MK_8	SK_{110}	8	$X_6^{29} \boxminus (F_1(X_5^{29}) \oplus SK_{110}) \to X_5^{28}$	$V_7[X_{4(0)}^9 \| X_7^{29} \| X_5^{29} \| X_5^{28} \| X_3^{28}]$	33	$2^{33} \cdot 2^{73}$
10	MK_{11}	SK_{105}	8	$X_5^{29} \oplus (F_0(X_3^{28}) \boxplus SK_{105}) \to X_3^{27}$	$V_8[X_{4(0)}^9 \| X_7^{29} \| X_5^{28} \| X_3^{27}]$	25	$2^{33} \cdot 2^{81}$
11	$MK_{12(7\sim1)}{}^*$	$SK_{106(7\sim1)}$	7	$X_7^{29} \boxminus (F_1(X_5^{28}) \oplus SK_{106}) \to X_5^{27}$	$V_9[X_{4(0)}^9 \| X_5^{28} \| X_5^{27} \| X_3^{27}]$	25	$2^{25} \cdot 2^{88}$
12	MK_7	SK_{101}	8	$X_5^{28} \oplus (F_0(X_3^{27}) \boxplus SK_{101}) \to X_3^{26}$	$V_{10}[X_{4(0)}^9 \| X_5^{27} \| X_3^{26}]$	17	$2^{117\ddagger}$
13	MK_3	SK_{97}	0	$X_5^{27} \oplus (F_0(X_3^{26}) \boxplus SK_{101}) \to X_3^{25}$	$V_{11}[X_{4(0)}^9 \| X_3^{25}]$	9	$2^{17} \cdot 2^{96}$

* $(7 \sim 1)$ denote the seven most significant bits, the least significant bit is guessed during the encryption phase.
† Measured in one computation of $\boxplus$ or $\oplus$, instead of 1/4 round encryption.
‡ The details of this step are shown in Table 5 and explained in the maintext.

Table 5
Detailed procedure for Step 12 of Table 4.

Step	Guess	Known key	#Bits	Computing	Counter	Size	Comp.
12-1	$MK_{7(0)}$	$SK_{101(0)}$	1	$X_{5(0)}^{28} \oplus (F_0(X_3^{27})_{(0)} \boxplus SK_{101(0)}) \to X_{3(0)}^{26}$	$V_{10}^1[X_{4(0)}^9 \| X_{5(7\sim1)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim1)} \| X_{3(0)}^{26}]^*$	24	$2^{25} \cdot 2^{89}$
12-2	$MK_{7(1)}$	$SK_{101(1)}$	1	$X_{5(1)}^{28} \oplus (F_0(X_3^{27})_{(1)} \boxplus SK_{101(1)}) \to X_{3(1)}^{26}$	$V_{10}^2[X_{4(0)}^9 \| X_{5(7\sim2)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim2)} \| X_{3(1\sim0)}^{26}]$	23	$2^{24} \cdot 2^{90}$
12-3	$MK_{7(2)}$	$SK_{101(2)}$	1	$X_{5(2)}^{28} \oplus (F_0(X_3^{27})_{(2)} \boxplus SK_{101(2)}) \to X_{3(2)}^{26}$	$V_{10}^3[X_{4(0)}^9 \| X_{5(7\sim3)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim3)} \| X_{3(2\sim0)}^{26}]$	22	$2^{23} \cdot 2^{91}$
12-4	$MK_{7(3)}$	$SK_{101(3)}$	1	$X_{5(3)}^{28} \oplus (F_0(X_3^{27})_{(3)} \boxplus SK_{101(3)}) \to X_{3(3)}^{26}$	$V_{10}^4[X_{4(0)}^9 \| X_{5(7\sim4)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim4)} \| X_{3(3\sim0)}^{26}]$	21	$2^{22} \cdot 2^{92}$
12-5	$MK_{7(4)}$	$SK_{101(4)}$	1	$X_{5(4)}^{28} \oplus (F_0(X_3^{27})_{(4)} \boxplus SK_{101(4)}) \to X_{3(4)}^{26}$	$V_{10}^5[X_{4(0)}^9 \| X_{5(7\sim5)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim5)} \| X_{3(4\sim0)}^{26}]$	20	$2^{21} \cdot 2^{93}$
12-6	$MK_{7(5)}$	$SK_{101(5)}$	1	$X_{5(5)}^{28} \oplus (F_0(X_3^{27})_{(5)} \boxplus SK_{101(5)}) \to X_{3(5)}^{26}$	$V_{10}^6[X_{4(0)}^9 \| X_{5(7\sim6)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7\sim6)} \| X_{3(5\sim0)}^{26}]$	19	$2^{20} \cdot 2^{94}$
12-7	$MK_{7(6)}$	$SK_{101(6)}$	1	$X_{5(6)}^{28} \oplus (F_0(X_3^{27})_{(6)} \boxplus SK_{101(6)}) \to X_{3(6)}^{26}$	$V_{10}^7[X_{4(0)}^9 \| X_{5(7)}^{28} \| X_5^{27} \| F_0(X_3^{27})_{(7)} \| X_{3(6\sim0)}^{26}]$	18	$2^{19} \cdot 2^{95}$
12-8	$MK_{7(7)}$	$SK_{101(7)}$	1	$X_{5(7)}^{28} \oplus (F_0(X_3^{27})_{(7)} \boxplus SK_{101(7)}) \to X_{3(7)}^{26}$	$V_{10}[X_{4(0)}^9 \| X_5^{27} \| X_3^{26}] = V_{10}^8[X_{4(0)}^9 \| X_5^{27} \| X_3^{26}]$	17	$2^{18} \cdot 2^{96}$

* Note that the computation $F_0(X_3^{27})_{(0)} \boxplus SK_{101(0)}$ could generate a carry bit, which is added to $F_0(X_3^{27})_{(7\sim1)}$. The value of $F_0(X_3^{27})_{(7\sim1)}$ that counter vector V_{10}^1 is counting here has been updated by this carry bit. The following steps in this table are done in a similar way.

have the same meaning as those in Table 4. According to Table 5, the time complexity for Step 12 of Table 4 is $2^{25} \cdot 2^{89} + 2^{24} \cdot 2^{90} + 2^{23} \cdot 2^{91} + 2^{22} \cdot 2^{92} + 2^{21} \cdot 2^{93} + 2^{20} \cdot 2^{94} + 2^{19} \cdot 2^{95} + 2^{18} \cdot 2^{96} = 8 \cdot 2^{114} = 2^{117}$ 1/4 round encryptions.

After Step 13 of Table 4, 96 master key bits have been guessed and the parity of $\alpha \diamond X^9 \oplus \beta \diamond X^{25}$ could be evaluated for all zero-correlation linear approximations presented in Table 3. Then we proceed the following steps:

14. Allocate a counter vector $V[z]$ of size 2^7 where each element is 64-bit length for 7-bit z (z is the concatenation of evaluations of 7 basis zero-correlation masks).
15. For 2^9 values of $(X_{4(0)}^9 | X_3^{25})$, evaluate all 7 basis zero-correlation masks with value $(X_{4(0)}^9 | X_3^{25})$ and put the evaluations to the vector z, then $V[z]$: $V[z] += V_{11}[X_{4(0)}^9 | X_3^{25}]$.
16. Compute $T = N \cdot 2^7 \cdot \sum_{z=0}^{2^7-1} (\frac{V[z]}{N} - \frac{1}{2^7})^2$, if $T \leqslant \tau$, then the guessed key is a possible key candidate. As there are 32 master key bits that we haven't guessed, we do exhaustive search for all keys conforming to this possible key candidate. Only the right key value will survive if all possible key values are tested against a maximum of 3 plaintext-ciphertext pairs.

4.1.1. Complexity estimation

In this attack, we set the type-I error probability $\alpha_0 = 2^{-2.7}$ and the type-II error probability $\alpha_1 = 2^{-8.9}$. We have $q_{1-\alpha_0} \approx 1.02$, $q_{1-\alpha_1} \approx 2.86$, $n = 64$, $\ell = 128$. Then N should satisfy

$$N = \frac{(2^n - 1)(q_{1-\alpha_0} + q_{1-\alpha_1})}{\sqrt{(\ell - 1)/2} + q_{1-\alpha_0}} + 1 \approx 2^{62.79}.$$

The decision threshold $\tau \approx 2^{6.35}$. There are 96-bit master key value guessed during the encryption and decryption phase, and $2^{96} \cdot 2^{-8.9} = 2^{87.1}$ key candidates survive in the wrong key filtration. These $2^{87.1}$ key candidates are tested exhaustively against a maximum of 3 plaintext-ciphertext pairs along with the remaining 32 master key bits. The complexity of Step 16 is about $2^{119.1}$ 26-round HIGHT encryptions which is also the dominant part of our attack. In total, the data complexity is about $2^{62.79}$ known plaintexts, the time complexity is about $2^{119.1}$ 26-round HIGHT encryptions and the memory requirement are 2^{43} bytes for counters. This is the first attack on 26-round HIGHT considering full whitening key with practical memory requirements.

Table 6
Decryption procedure of the attack on 27-round HIGHT.

Step	Guess	Known key	#Bits	Computing	Counter	Size	Comp.
4	$MK_{3(7\sim1)}$	$WK_{7(7\sim1)}$	7	$C_6 \oplus WK_7 \rightarrow X_6^{30}$	$V_2[X_{4(0)}^9 \| C_7 \| C_0 \| X_6^{30} \| X_5^{30} \| X_3^{29}]$	41	$2^{41} \cdot 2^{65}$
5	MK_0	SK_{119}	8	$C_7 \oplus (F_0(X_6^{30}) \boxplus SK_{119}) \rightarrow X_7^{30}$	$V_3[X_{4(0)}^9 \| C_0 \| X_7^{30} \| X_6^{30} \| X_5^{30} \| X_3^{29}]$	41	$2^{41} \cdot 2^{73}$
6	MK_3	SK_{114}	0	$X_6^{30} \boxminus (F_1(X_5^{30}) \oplus SK_{114}) \rightarrow X_5^{29}$	$V_4[X_{4(0)}^9 \| C_0 \| X_7^{30} \| X_5^{30} \| X_5^{29} \| X_3^{29}]$	41	$2^{41} \cdot 2^{73}$
7	MK_{15}	SK_{109}	0	$X_5^{30} \oplus (F_0(X_3^{29}) \boxplus SK_{109}) \rightarrow X_3^{28}$	$V_5[X_{4(0)}^9 \| C_0 \| X_7^{30} \| X_5^{29} \| X_3^{28}]$	33	$2^{41} \cdot 2^{73}$
8	MK_0	WK_4	0	$C_0 \boxplus WK_4 \rightarrow X_0^{30}$	$V_6[X_{4(0)}^9 \| X_7^{30} \| X_0^{30} \| X_5^{29} \| X_3^{28}]$	33	$2^{33} \cdot 2^{73}$
9	MK_4	SK_{115}	8	$X_0^{30} \oplus (F_0(X_7^{30}) \boxplus SK_{115}) \rightarrow X_7^{29}$	$V_7[X_{4(0)}^9 \| X_7^{30} \| X_7^{29} \| X_5^{29} \| X_3^{28}]$	33	$2^{33} \cdot 2^{81}$
10	MK_8	SK_{110}	8	$X_7^{30} \boxminus (F_1(X_5^{29}) \oplus SK_{110}) \rightarrow X_5^{28}$	$V_8[X_{4(0)}^9 \| X_7^{29} \| X_5^{29} \| X_5^{28} \| X_3^{28}]$	33	$2^{33} \cdot 2^{89}$
11	MK_{11}*	SK_{105}	8	$X_5^{29} \oplus (F_0(X_3^{28}) \boxplus SK_{105}) \rightarrow X_3^{27}$	$V_9[X_{4(0)}^9 \| X_7^{29} \| X_5^{28} \| X_3^{27}]$	25	2^{126}
12	$MK_{12(7\sim1)}$*	$SK_{106(7\sim1)}$	7	$X_7^{29} \boxminus (F_1(X_5^{28}) \oplus SK_{106}) \rightarrow X_5^{27}$	$V_{10}[X_{4(0)}^9 \| X_5^{28} \| X_5^{27} \| X_3^{27}]$	25	2^{125}
13	MK_7*	SK_{101}	0	$X_5^{28} \oplus (F_0(X_3^{27}) \boxplus SK_{101}) \rightarrow X_3^{26}$	$V_{11}[X_{4(0)}^9 \| X_5^{27} \| X_3^{26}]$	17	2^{125}
14	MK_3	SK_{197}	0	$X_5^{27} \oplus (F_0(X_3^{26}) \boxplus SK_{97}) \rightarrow X_3^{25}$	$V_{12}[X_{4(0)}^9 \| X_3^{25}]$	9	$2^{17} \cdot 2^{104}$

* The key bytes of MK_{11}, MK_{12}, MK_7 are guessed bit by bit from the least significant bit to the most significant bit, respectively. The complexities could be calculated in a similar way as described in the attack on 26-round HIGHT. Note that extra counters needed during this procedure are not listed.

4.2. Key-recovery attack on 27-round HIGHT

If we add one more round after the zero-correlation linear distinguisher for 16-round HIGHT, we could attack 27-round HIGHT (round 4 to round 30) with full whitening key taken into consideration. The initial five rounds encryption of our attack on 27-round HIGHT is the same as that described in Section 4.1 shown in Fig. 1. The final six rounds are illustrated in Fig. 3. The key-recovery phase could be proceeded with partial-sum technique from Step 1 to Step 17 as follows.

1. Allocate a counter vector $V_1[X_{4(0)}^9 \| C_7 \| C_6 \| C_0 \| X_5^{30} \| X_3^{29}]$ of size 2^{41} where each element is 32-bit length and initialize to zero.
2. Guess all possible values of 58 master key bits MK_{15}, MK_{14}, MK_{13}, MK_2, MK_1, MK_6, $MK_{3(0)}$, $MK_{12(0)}$, MK_7.
3. Partially encrypt and decrypt each of N (P, C) pairs to get $X_{4(0)}^9$, X_5^{30} and X_3^{29}. Add one to corresponding $V_1[X_{4(0)}^9 \| C_7 \| C_6 \| C_0 \| X_5^{30} \| X_3^{29}]$.

The time complexity of Step 3 is no more than $N \cdot 2^{58} \cdot \frac{5}{27}$ 27-round encryptions. Then, we proceed Steps 4–14 shown in Table 6. The meaning of each column in Table 6 has already been described in Section 4.1. Also, Step 4 to Step 14 of Table 6 are proceeded in the same way as described in Section 4.1.

After Step 14 of Table 6, 104 master key bits have been guessed and the parity of $\alpha \diamond X^9 \oplus \beta \diamond X^{25}$ could be evaluated for all zero-correlation linear approximations shown in Table 3. Then we proceed the following steps:

15. Allocate a counter vector $V[z]$ of size 2^7 where each element is 64-bit length for 7-bit z (z is the concatenation of evaluations of 7 basis zero-correlation masks).
16. For 2^9 values of $(X_{4(0)}^9 \| X_3^{25})$, evaluate all 7 basis zero-correlation masks on $(X_{4(0)}^9 \| X_3^{25})$ and put the evaluations to the vector z, then add the corresponding $V[z]$: $V[z] += V_{12}[X_{4(0)}^9 \| X_3^{25}]$.
17. Compute $T = N \cdot 2^7 \cdot \sum_{z=0}^{2^7-1} (\frac{V[z]}{N} - \frac{1}{2^7})^2$, if $T \leqslant \tau$, then the guessed key is a possible key candidate. As there are 24 master key bits that we haven't guessed, we do exhaustive search for all keys conforming to this possible key candidate. Only the right key value will survive if each possible key value is tested against a maximum of 3 plaintext-ciphertext pairs.

4.2.1. Complexity estimation

In this attack, we also choose $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-8.9}$. Again $q_{1-\alpha_0} \approx 1.02$, $q_{1-\alpha_1} \approx 2.86$, $n = 64$, $\ell = 127$ and N should satisfy

$$N = \frac{(2^n - 1)(q_{1-\alpha_0} + q_{1-\alpha_1})}{\sqrt{(\ell - 1)/2} + q_{1-\alpha_0}} + 1 \approx 2^{62.79}.$$

About $2^{104} \cdot 2^{-8.9} = 2^{95.1}$ candidates are left after filtration, the complexity of the test in Step 17 is about $2^{95.1} \cdot 2^{24} = 2^{119.1}$ 27-round encryptions. Note that Steps 11, 12, 13 in Table 6 have comparable time complexity. So the time complexity of our attack on 27-round HIGHT is about $(2^{126} + 2^{125} + 2^{125}) \cdot \frac{1}{4} \cdot \frac{1}{27} + 2^{119.1} \approx 2^{120.78}$ 27-round encryptions. The data complexity is $2^{62.79}$ known plaintexts and the required memory is about 2^{43} bytes. Compared with the previous best attack proposed in [14], our attack on 27-round HIGHT has a lower time complexity and successfully eliminates the requirements for unpractical memory.

5. Conclusion

In this paper, we evaluate the security of HIGHT with respect to the novel technique of multidimensional zero-correlation cryptanalysis. As a result, we can attack 27 rounds of HIGHT in less time with a practical memory complexity. We also propose the first single-key cryptanalysis of 26-round HIGHT with all whitening keys. Thus, our 27-round attack improves upon the state-of-the-art cryptanalysis for HIGHT and is the best non-exhaustive single-key cryptanalysis of ISO standard HIGHT to date.

Acknowledgements

This work has been supported by 973 program (No. 2013CB834205), NSFC Projects (No. 61133013 and No. 61070244), Program for New Century Excellent Talents in University of China (No. NCET-13-0350), as well as Interdisciplinary Research Foundation of Shandong University (No. 2012JC018).

References

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, The SIMON and SPECK families of lightweight block ciphers, Cryptology ePrint Archive, Report 2013/404, 2013.

[2] A. Bogdanov, G. Leander, K. Nyberg, M. Wang, Integral and multidimensional linear distinguishers with correlation zero, in: X. Wang, K. Sako (Eds.), AsiaCrypt 2012, in: Lect. Notes Comput. Sci., vol. 7658, Springer, Heidelberg, 2012, pp. 24–262.

[3] A. Bogdanov, H. Geng, M. Wang, L. Wen, B. Collard, Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA, in: T. Lange, K. Lauter, P. Lisonek (Eds.), SAC'13, in: Lect. Notes Comput. Sci., Springer-Verlag, 2013, in press.

[4] A. Bogdanov, V. Rijmen, Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography, Springer, US, 2012, pp. 1–15.

[5] A. Bogdanov, M. Wang, Zero Correlation Linear Cryptanalysis with Reduced Data Complexity, in: A. Canteaut (Ed.), FSE 2012, in: Lect. Notes Comput. Sci., vol. 7549, Springer, Heidelberg, 2012, pp. 29–48.

[6] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, S. Chee, HIGHT: A new block cipher suitable for low-resource device, in: L. Goubin, M. Matsui (Eds.), CHES 2006, in: Lect. Notes Comput. Sci., vol. 4249, Springer, Heidelberg, 2006, pp. 46–59.

[7] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, in: P. Paillier, I. Verbauwhede (Eds.), CHES 2007, in: Lect. Notes Comput. Sci., vol. 4727, Springer, Heidelberg, 2007, pp. 450–466.

[8] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, The 128-bit blockcipher CLEFIA (extended abstract), in: A. Biryukov (Ed.), FSE 2007, in: Lect. Notes Comput. Sci., vol. 4593, Springer, Heidelberg, 2007, pp. 181–195.

[9] International Organization for Standardization. ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, 2010.

[10] P. Zhang, B. Sun, C. Li, Saturation attack on the block cipher HIGHT, in: J.A. Garay, A. Miyaji, A. Otsuka (Eds.), CANS 2009, in: Lect. Notes Comput. Sci., vol. 5888, Springer, Heidelberg, 2009, pp. 76–86.

[11] Y. Sasaki, L. Wang, Meet-in-the-Middle technique for integral attacks against Feistel ciphers, in: L.R. Knudsen, H. Wu (Eds.), SAC 2012, in: Lect. Notes Comput. Sci., vol. 7707, Springer, Heidelberg, 2013, pp. 234–251.

[12] J. Lu, Cryptanalysis of reduced versions of the HIGHT block cipher from CHES 2006, in: K.-H. Nam, G. Rhee (Eds.), ICISC 2007, in: Lect. Notes Comput. Sci., vol. 4817, Springer, Heidelberg, 2007, pp. 11–26.

[13] O. Özen, K. Varici, C. Tezcan, Ç. Kocair, Lightweight block ciphers revisited: Cryptanalysis of reduced round PRESENT and HIGHT, in: C. Boyd, J.G. Nieto (Eds.), ACISP 2009, in: Lect. Notes Comput. Sci., vol. 5594, Springer, Heidelberg, 2009, pp. 90–107.

[14] J. Chen, M. Wang, B. Preneel, Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT, in: A. Mitrokotsa, S. Vaudenay (Eds.), AfricaCrypt 2012, in: Lect. Notes Comput. Sci., vol. 7374, Springer, Heidelberg, 2012, pp. 117–137.

[15] D. Hong, B. Koo, D. Kwon, Biclique attack on the full HIGHT, in: H. Kim (Ed.), ICISC 2011, in: Lect. Notes Comput. Sci., vol. 7259, Springer, Heidelberg, 2011, pp. 365–374.

[16] J. Song, K. Lee, H. Lee, Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo, Int. J. Comput. Math. (2013) 1–16.

[17] B. Koo, D. Hong, D. Kwon, Related-key attack on the full HIGHT, in: K.-H. Rhee, D. Nyang (Eds.), ICISC 2010, in: Lect. Notes Comput. Sci., vol. 6829, Springer, Heidelberg, 2011, pp. 49–67.